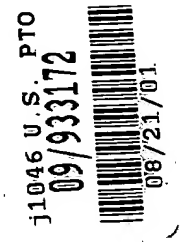
#2

Atty. Dkt. No. 072982-0225

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Applicant: Akihisa TOMITA

Title: CRYPTOGRAPHIC KEY DISTRIBUTION METHOD AND APPARATUS THEREOF

Appl. No.: Unassigned

Filing Date: August 21, 2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japanese Patent Application No. 2000-252656 filed August 23, 2000.

Respectfully submitted,

Date August 21, 2001

By Phillip J. Articola
for / David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

Reg. No. 38819

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　８月２３日

出願番号
Application Number: 特願２０００－２５２６５６

出願人
Applicant(s): 日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　６月２０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　34103562
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/38
　　H04B 10/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　富田　章久
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100082935
　【弁理士】
　【氏名又は名称】　京本　直樹
　【電話番号】　03-3454-1111
【選任した代理人】
　【識別番号】　100082924
　【弁理士】
　【氏名又は名称】　福田　修一
　【電話番号】　03-3454-1111
【選任した代理人】
　【識別番号】　100085268
　【弁理士】
　【氏名又は名称】　河合　信明
　【電話番号】　03-3454-1111
【手数料の表示】
　【予納台帳番号】　008279

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9115699

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　暗号鍵配布方法及び装置

【特許請求の範囲】

【請求項１】　送信者は、送信端で盗聴者がいかなる受信機で盗聴したときでも盗聴者の信号対雑音比が２ｄＢ以下になり、且つ、受信端における受信者の信号対雑音比が－１０ｄＢ以上になるように出力信号光の光強度と変調度を設定し、乱数列を符号化した変調信号で変調した信号光を送信し、受信者は、一連の乱数列の信号光を受信した後、雑音重畳に由来した揺らぎを有する受信信号の頻度分布から確率分布を計算して、前記確率分布の変化に基づいて盗聴の有無を判別すると共に、受信者の誤り率が５％以下になるように判別閾値を設定して、前記判別閾値に基づいて乱数列の各ビットのビット値を判別し、判別できたビットの位置を送信者に連絡して判別誤りのないビット列のみを取り出して送信者と共有し、前記共有したビット列を暗号鍵とすることを特徴とする暗号鍵配布方法。

【請求項２】　乱数は２値乱数とし、受信側で２値に相当する２つのピークを有し、互いに対称な確率分布になるように２値の乱数列を符号化することを特徴とする請求項１記載の暗号鍵配布方法。

【請求項３】　２値乱数の符号化にマンチェスター符号を用いたことを特徴とする請求項２記載の暗号鍵配布方法。

【請求項４】　計算した確率分布が２値（０，１）に相当する対称形をなす２つのピークを有することを確認し、そのような確率分布が確認できない場合は、暗号鍵配布において盗聴があったと判断して、暗号鍵の配布をやり直すことを特徴とする請求項１～３の何れかに記載の暗号鍵配布方式。

【請求項５】　暗号鍵伝送に際し、暗号鍵伝送路とは独立な通信路を用いて、管理情報として、クロック、及び、送信信号光の光強度と変調度を受信者に送信することを特徴とする請求項１～４の何れかに記載の暗号鍵配布方法。

【請求項６】　受信者は、受信した送信側の光強度情報と既知の伝送路損失から推定される受信光の光強度期待値を計算し、その結果と実際に受信した受信光の光強度とを比較し、計算値と実測値との差に応じて伝送路の異常程度を判断し、それを手がかりに暗号鍵配布の中止を決定することを特徴とする請求項５記

載の暗号鍵配布方式。

【請求項７】　符号化された乱数列で変調された信号光を出射する送信装置と、前記送信装置からの前記信号光を伝送する伝送路と、前記伝送路からの信号光を受信・復号し、雑音重畳に由来した揺らぎのある復号信号の頻度分布から確率分布を計算して、前記確率分布の変化に基づいて盗聴の有無を判別すると共に、誤り率が５％以下になるように判別閾値を設定して、前記判別閾値に基づいて乱数列の各ビットのビット値を判別し、判別できたビットの位置を送信者に送信する受信装置とから成り、前記送信装置を出射する信号光の１パルス当たりの平均光子数Ｎ（Ｎ≧１）及び変調度δと前記伝送路の伝送損失Ｌとが下記式を満足することを特徴とする暗号鍵配布装置。

$\delta \leqq 0.8/N$

$2\delta L^2N^2/Nn > 0.1$

ここで、Ｎｎは受信装置の雑音レベルである。

【請求項８】　送信装置が、第１の光源と、クロック発生器と、前記クロック発生器のクロックに基づいて乱数を発生する乱数発生器と、前記乱数発生器で発生した乱数を符号化する符号化器と、前記符号化器からの信号に基づいて第１の光源からの光を変調して信号光とする第１の変調器と、前記第１の変調器からの信号光を雑音レベル程度の光強度に減衰する減衰器と、クロック光に用いられる光を発生する第２の光源と、前記クロック発生器のクロックに基づいて第２の光源からの光を変調してクロック光とする第２の変調器と、前記減衰器から出射した信号光と前記前記第２の変調器から出射したクロック光とを合波して伝送路に出力する合波器とを有し、受信装置が、信号光とクロック光とを分離する波長分波器と、前記波長分波器からのクロック光を電気的なクロックに変換するクロック再生装置と、前記波長分波器から出射した信号光を復号して、電気信号に変換する復号・検出器と、前記クロック再生装置からのクロックに基づいて前記復号・検出器からの電気信号の頻度分布の計測、頻度分布に基づく確率分布の計算、前記確率分布の変化に基づいて盗聴の有無の判別、誤り率が５％以下になる判別閾値の設定、前記判別閾値に基づく乱数列の各ビットのビット値の判別、判別できたビット位置の送信を行う演算装置とを有することを特徴とする請求項７記

載の暗号鍵配布装置。

【請求項９】　クロック再生装置が、クロック光を光電変換する光検出器と、前記光検出器からの電気信号を波形整形するクロック再生回路とを含み、復号・検出器が、信号光を１対１に分岐する分波器と、前記分波器で２つに分岐した信号光の内の一方の信号光を遅延する遅延器と、前記遅延器を経た信号光と前記分波器からの他方の信号光との差を電気信号に変換するバランスドデテクタとを含むことを特徴とする請求項８記載の暗号鍵配布装置。

【請求項１０】　符号化器は、受信装置側で２値に相当する２つのピークを有し、互いに対称な確率分布が得られるように乱数列を符号化することを特徴とする請求項８又は９記載の暗号鍵配布装置。

【請求項１１】　乱数列の符号化にマンチェスター符号を用いたことを特徴とする請求項７～１０の何れかに記載の暗号鍵配布装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、秘匿性の高い情報通信に関し、特に盗聴者に対して物理法則を用いて秘匿性を保った暗号鍵の配布方法及び装置に関する。

【０００２】

【従来の技術】

送信者と受信者の間で情報を伝達する際に、二者が秘匿性の高い乱数の組（暗号鍵）を共有することによって、傍受されても安全な情報の伝達や、改ざんの防止が可能になる。秘匿性が高く、情報理論的に絶対的な安全性が証明されている暗号鍵、即ち、平文と同じ長さの暗号鍵を用いて情報を伝達する方法では、一度使った暗号鍵は必ず捨てるため、暗号鍵は一度しか用いることができず、常に新しい暗号鍵を配布する必要があり、非現実的である。

【０００３】

現実的で、暗号鍵配布方法の秘匿性を量子力学の原理に求めた量子暗号鍵配布方法として提案されている方法を用いると、安全な暗号鍵を送り手と受け手のみで共有でき、絶対的に安全な通信が可能になることが知られている。この量子暗

号鍵配布方法は、量子力学の法則によって、状態の基底をあらかじめ知らないかぎり量子状態を正確に測定できないことから、盗聴者の存在は伝送における誤りの増加として検出される。量子暗号鍵配布の具体的な方法はベネット（Ｂｅｎｎｅｔｔ，Ｃ．Ｈ．）とブラッサード（Ｂｒａｓｓａｒｄ，Ｇ．）によってＩＢＭテクニカルディスクロージャブリテン（ＩＢＭ　Ｔｅｃｈｎｉｃａｌ　ｄｉｓｃｌｏｓｕｒｅ　ｂｕｌｌｅｔｉｎ）２８巻３１５３－３１６３頁（１９８５）で提案された。ベネットは、より光ファイバによる伝送に適した非直交２状態を用いた方法もフィジカルレビューレターズ（Ｐｈｙｓｉｃａｌ　Ｒｅｖｉｅｗ　Ｌｅｔｔｅｒｓ）誌６８巻３１２１－３１２４頁に述べている。量子暗号は物理法則が暗号の安全性を保証するため、計算機の能力の限界に依存しない究極の安全性保証が可能になる。

【０００４】

【発明が解決しようとする課題】

しかしながら、上述した従来の量子暗号プロトコルでは１ビットの情報を１つの光子で送ることが必要である。このため、光の検出には量子効率の低い光子計数法を用いなければならず、伝送効率が小さい。また、光の偏光や位相に信号を載せているために伝送路での擾乱に弱く、誤り率が増大して安全な暗号伝送ができなることもあるといった問題がある。また、伝送路におけるコヒーレンスの必要性のため光増幅器を用いることができず、現在の光ファイバ通信網に用いることができず、専用線が必要になる。このため、敷設のコストが大きいという問題が生じる。

【０００５】

ベネット（Ｂｅｎｎｅｔｔ，Ｃ．Ｈ．）とウィズナー（Ｗｉｅｓｎｅｒ，Ｓ．Ｊ．）は合衆国特許第５，５１５，４３８号において非常に弱い変調をかけたコヒーレント光を用いる暗号鍵配布の方法を開示した。この方法では、たとえば、平均Ｎ個の光子を送るとき（“１”，“０”）に応じて（Ｎｃｏｓ２（π／４－δ），Ｎｃｏｓ２（π／４＋δ））と（Ｎｓｉｎ２（π／４－δ），Ｎｓｉｎ２（π／４＋δ））のように２種類の変調をかけた信号を用いる。このため、測定による揺らぎの大きさが変調の強さと同程度以上になるように変調指数（変調度

とも云う）δを小さな値に選ぶと、測定では状態を正確に決めることができなくなる。さらに、２つの独立な信号を用いることでベネット（Ｂｅｎｎｅｔｔ，Ｃ．Ｈ．）とブラッサード（Ｂｒａｓｓａｒｄ，Ｇ．）によって提案された４状態を用いた量子暗号と同様な安全性が期待できる。しかし、彼らのプロトコルでは１ビットの伝送に２つの信号を必要とする。さらに、これら２つの信号の間で位相コヒーレンスを保つ量子通信路を必要とし、その分擾乱に対して弱くなっている。

【０００６】

これに対してユーエン（Ｙｕｅｎ，Ｈ．Ｐ．）とキム（Ｋｉｍ，Ａ．Ｍ．）はフィジックスレターズ（Ｐｈｙｓｉｃｓ　Ｌｅｔｔｅｒｓ）誌Ａ２４１巻，１３５－１３８頁、（１９９８）で弱い多光子光（コヒーレント光）でも用いることのできる暗号鍵配布の具体的なプロトコルを与え、彼らのプロトコルが本質的には非直交２状態を用いた量子暗号と同様な原理によって安全性が保障されていることを示した。彼らの方法では伝送路でのコヒーレンスは必要とせず、現在の光ファイバ通信網の中で用いることができる。

【０００７】

ユーエンーキムのプロトコルでは”０”と”１”が対称的な確率分布で受信されるように符号化される。送信者　は符号化された信号を弱いコヒーレント光に乗せて伝送する。通常の通信ではＶ＝０を閾値として”０”と”１”を判別する。これに対してユーエンーキムのプロトコルでは$V_{th}=\pm mS$（Ｓは信号の振幅の平均値）をそれぞれ”１”、”０”に対する閾値とする。このため、受信した信号は非直交２状態を用いた量子暗号と同様に”１”、”０”、”判別不能”の３つに判別される。受信者は”判別不能”とされたビットの位置を送信者に伝え、このビットを捨てる。受信者が”１”か”０”に判別できたビット列には誤りが含まれているので送信者と受信者はビットを交換して誤りのないビット列を得る。送信者と受信者は誤り訂正を行った後、残ったビットからハッシュ関数による秘匿性の増強によって安全な暗号鍵を確立する。

【０００８】

ユーエンーキムのプロトコルはつぎのような性質を安全性の基礎にしている。

信号は弱いコヒーレント光で伝送されるため、信号対雑音比が悪く、閾値を０にすると無視できない割合で誤りが生じる。一方、閾値を上げると”判別不能”とされるビットが増えるが残ったビットの誤り率を十分小さくすることができる。盗聴者がいる場合、盗聴者は判別のための閾値を０にしなければならない。これは、受信者と盗聴者の信号に加わる雑音は互いに相関がないため、盗聴者の閾値が０でないと受信者が判別したビットを盗聴者も同時に判別できる確率が小さくなる。判別できなかったビットに対する情報量は０であり、閾値０で判別したときの誤りは０．５より小さいから盗聴者は閾値を０にして全てのビットについての情報を得た方が有利になる。このとき、受信者の得た誤りの少ないビットは盗聴者にとっては誤りを含んだものになる。このため、受信者の情報量に対して盗聴者の情報量は小さく、盗聴は失敗に終わる。また、盗聴者が送られる信号を全て吸収して判別した結果を受信者に再送するという攻撃を行ったとき、盗聴者の誤り率が１０％を越えていれば受信者側の誤り率の異常な増加として盗聴者の存在が検知できる。

【０００９】

しかし、盗聴者が送信者の極めて近くにいる場合には盗聴者の信号対雑音比が良いため閾値を０で判別を行っても盗聴者の得るビットの誤りが小さくなる。このような場合には盗聴が可能になるため、システムの設計を行うには理論上安全性が保証できる盗聴者の信号対雑音比の限度が明らかになっている必要がある。ユーエンとキムの報告ではこの点についての考察がなされておらず、盗聴者が存在しても安全な暗号鍵配布が行えるシステム設計を行う上で問題があった。また、盗聴者が０でない閾値で判別を行い、判別できたビットだけを受信者に再送する攻撃を行うとき、再送する信号を強くすれば受信される平均光子数は盗聴がない場合と変わらず、受信者側の誤りを減らすことができるため盗聴が成功しやすくなるという問題がある。また、平野は特開２０００－１０１５７０号公報においてユーエン－キムと同様な原理に基づく暗号システムを開示しているが、ここでも盗聴者の信号対雑音比についての考察はなされていない。

【００１０】

本発明の目的は、量子通信路を必要とせず、現在の光通信網を利用できる安全

な暗号鍵配布方法と装置を提供することにある。

【００１１】

【課題を解決するための手段】

本発明の暗号鍵配布方法は、送信端で盗聴者がいかなる受信機で盗聴したときでも盗聴者の信号対雑音比が２ｄＢ以下になり、且つ、受信端における受信者の信号対雑音比が－１０ｄＢ以上になるように出力信号光の光強度と変調度を設定し、乱数列を符号化した変調信号で変調した信号光を受信者に伝送し、受信者は、一連の乱数列の信号光を受信した後、雑音重畳に由来した揺らぎを有する受信信号の頻度分布から確率分布を計算して、前記確率分布の変化に基づいて盗聴の有無を判別すると共に、受信者の誤り率が５％以下になるように判別閾値を設定して、前記判別閾値に基づいて乱数列の各ビットのビット値を判別し、判別できたビットの位置を送信者に連絡して判別誤りのないビット列のみを取り出して送信者と共有し、前記共有したビット列を暗号鍵とすることを特徴としている。

【００１２】

上記暗号鍵配布方法は、下記（１）～（５）の少なくとも１つを特徴として含んでいてもよい。

（１）乱数は２値乱数とし、受信側で２値に相当する２つのピークを有し、互いに対称な確率分布になるように２値の乱数列を符号化する。

（２）２値乱数の符号化にマンチェスター符号を用いる。

（３）計算した確率分布が２値（０，１）に相当する対称形をなす２つのピークを有することを確認し、そのような確率分布が確認できない場合は、暗号鍵配布において盗聴があったと判断して、暗号鍵の配布をやり直す。

（４）暗号鍵伝送に際し、暗号鍵伝送路とは独立な伝送路を用いて、管理情報として、クロック、及び、送信信号光の光強度と変調度を受信者に送信する。

（５）受信者は、受信した送信側の光強度情報と既知の伝送路損失から推定される受信光の光強度期待値を計算し、その結果と実際に受信した受信光の光強度とを比較し、計算値と実測値との差に応じて伝送路の異常程度を判断し、それを手がかりに暗号鍵配布の中止を決定する。

【００１３】

本発明の暗号鍵配布装置は、符号化された乱数列で変調された信号光を出射する送信装置と、前記送信装置からの前記信号光を伝送する伝送路と、前記伝送路からの信号光を受信・復号し、雑音重畳に由来した揺らぎのある復号信号の頻度分布から確率分布を計算して、前記確率分布の変化に基づいて盗聴の有無を判別すると共に、誤り率が５％以下になるように判別閾値を設定して、前記判別閾値に基づいて乱数列の各ビットのビット値を判別し、判別できたビットの位置を送信者に送信する受信装置とから成り、前記送信装置を出射する信号光の１パルス当たりの平均光子数Ｎ（Ｎ≧１）及び変調度δと前記伝送路の伝送損失Ｌとが下記式１、式２を満足することを特徴としている。

［式１］　$\delta \leqq 0.8/N$

［式２］　$2\delta L^2N^2/Nn > 0.1$

ここで、Ｎｎは受信装置の雑音レベルで、予め測定して求めておけばよい。

【００１４】

本発明の暗号鍵配布装置は、上記式１、式２を満たすことで、送信端で盗聴者がいかなる受信機で盗聴したときでも盗聴者の信号対雑音比が２ｄＢ以下になり、且つ、受信端における受信者の信号対雑音比が－１０ｄＢ以上になり、盗聴に対して安全に暗号鍵を配布できる。

【００１５】

上記暗号鍵配布装置は、より具体的には、送信装置が、第１の光源と、クロック発生器と、前記クロック発生器のクロックに基づいて乱数を発生する乱数発生器と、前記乱数発生器で発生した乱数を符号化する符号化器と、前記符号化器からの信号に基づいて第１の光源からの光を変調して信号光とする第１の変調器と、前記第１の変調器からの信号光を雑音レベル程度の光強度に減衰する減衰器と、クロック光に用いられる光を発生する第２の光源と、前記クロック発生器のクロックに基づいて第２の光源からの光を変調してクロック光とする第２の変調器と、前記減衰器から出射した信号光と前記前記第２の変調器から出射したクロック光とを合波して伝送路に出力する合波器とを有し、受信装置が、信号光とクロック光とを分離する波長分波器と、前記波長分波器からのクロック光を電気的なクロックに変換するクロック再生装置と、前記波長分波器から出射した信号光を

復号して、電気信号に変換する復号・検出器と、前記クロック再生装置からのクロックに基づいて前記復号・検出器からの電気信号の頻度分布の計測、頻度分布に基づく確率分布の計算、前記確率分布の変化に基づいて盗聴の有無の判別、誤り率が５％以下になる判別閾値の設定、前記判別閾値に基づく乱数列の各ビットのビット値の判別、判別できたビット位置の送信を行う演算装置とを有する構成とするのが望ましい。また、クロック再生装置が、クロック光を光電変換する光検出器と、前記光検出器からの電気信号を波形整形するクロック再生回路とを含み、復号・検出器が、信号光を１対１に分岐する分波器と、前記分波器で２つに分岐した信号光の内の一方の信号光を遅延する遅延器と、前記遅延器を経た信号光と前記分波器からの他方の信号光との差を電気信号に変換するバランスドデテクタとを含む構成とし、符号化器は、受信装置側で２値に相当する２つのピークを有し、互いに対称な確率分布が得られるように乱数列を符号化するのがよい。具体的には、マンチェスター符号を用いるとよい。ここで、乱数は２値乱数とし、受信側で２値に相当する２つのピークを有し、互いに対称な確率分布になるように符号化しているのは、２値（０，１）の判別の際に、量子暗号と同様に、”０”、”１”、”判別不能”の３つの判別状態が得られるようにして、盗聴に対して安全に暗号鍵を配布できるようにするためである。

【００１６】

本発明の元となった研究によれば、盗聴者の誤り率が１０％を越えているとき、受信者の信号対雑音比の盗聴者からの劣化が１２ｄＢ以下であれば安全な暗号鍵配布ができることが明らかになった。盗聴者が送信者に隣接し最良の受信機を用いたとき、盗聴者の信号対雑音比は最良になる。この条件においても盗聴者の信号対雑音比が２ｄＢ以下であれば、盗聴者の用いる閾値が０であるとき誤り率は１０％以上になる。そこで、受信者の信号対雑音比が－１０ｄＢ以上になるように伝送路の損失と送信信号光の光強度及び変調度が設計されていれば受信者の誤り率を５％以下にすることができ、安全な暗号鍵配布ができる。従って、このような条件が満たされる限り共有された暗号鍵の安全性を保証することができる。また、クロックの伝送は送受信機の同期に必要であり、送信側の光強度と変調度を送って受信側で予想される値と比較することにより受信側で、盗聴者が一部

のビットだけを強い光で再送した場合などの伝送路の異常を検知できる。このため、コヒーレント光による、現在の光通信網を利用できる安全な暗号鍵配布システムが実現される。

【００１７】

また、本発明における受信側での閾値の設定は、受信者が検出した信号の振幅から誤り率が所要の値より小さくなるように判別閾値を設定して判別を行ってもよい。

【００１８】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して詳細に説明する。

【００１９】

図１を参照すると、本発明の一実施の形態としての構成図が示されている。図１において、送信者側の装置はクロック発生器（１１）、乱数発生器（１２）、符号化器（１３）、第１の光源（１４）、第１の変調器（１５）、減衰器（１６）、光強度モニタ（１７）、第２の光源（１８）、第２の変調器（１９）と合波器（１１０）からなる。第１の光源（１４）と第２の光源（１８）の波長は異なっている。送信者側と受信者側は光を伝送路（１１１）で結ばれている。受信者側の装置は波長分波器（１１２）、クロック再生装置（１１３）、復号・検出器（１１４）と演算装置（１１５）から成る。演算装置（１１５）には記憶装置（１１６）が接続されている。復号・検出器（１１４）は５０％－５０％（分岐比が１対１）の分波器（１１７）と遅延器（１１８）、バランスドデテクタ（１１９）、増幅器（１２０）から成る。クロック再生装置（１１３）は光検出器（１２１）とクロック再生回路（１２２）から成る。ここで、光源、変調器等各部品は既存のものが利用できる。その主なものの一例を示すと、第１、第２の光源は半導体レーザ等が利用できる。第１、第２の変調器は、ポッケルスセル等の電気光学素子やファラデー素子等の磁気光学素子が利用できるが、半導体レーザと同じ材料を用いた電界吸収型光変調器を用いると、同一基板上に半導体レーザとモノリシックに集積化できる利点があるので、半導体電界吸収型光変調器を用いるのがよい。合波器（１１０）は、Ｙ字型分岐導波路や多モード干渉導波路等が、

波長分波器（１１２）には、アレイ導波路格子やフォトニック結晶を用いたもの等が、分波器（１１７）には、方向性結合器等が、遅延器（１１８）は光ファイバ等が利用できる。また、クロック再生回路（１２２）は、光検出器（１２１）で得られた波形を矩形に整形すればよいから既存の波形整形回路が利用できる。演算装置（１１５）はマイクロコンピュータやパーソナルコンピュータが利用できる。パーソナルコンピュータを用いた場合は記憶装置はパーソナルコンピュータに内蔵されているので、記憶装置（１１６）を演算装置（１１５）と独立に設ける必要はない。ここで、演算装置（１１５）は、図７、図８に示す流れ図に従って動作する。

【００２０】

乱数発生器（１２）はクロック発生器（１１）からクロック信号が送られるごとに一定個数の２値乱数を発生する。得られた乱数は符号化器（１３）によって立上りを“０”立下りを“１”とするマンチェスター符号に符号化される。符号化された乱数は第１の変調器（１５）を介して第１の光源（１４）の光出力を変調する。クロック信号はまた、第１の光源（１４）とは異なる波長の第２の光源（１８）の光を第２の変調器を介して変調する。乱数信号で変調された光出力は減衰器（１６）によって減衰され、光強度が雑音レベル程度の微弱な信号光になる。この減衰した信号光の光強度は下記式１、式２を満足する。この結果、送信端で盗聴者がいかなる受信機で盗聴したときでも盗聴者の信号対雑音比が２ｄＢ以下になり、且つ、受信端における受信者の信号対雑音比が－１０ｄＢ以上になる。乱数信号で変調され、減衰器（１６）で減衰された出力光（信号光）とクロック信号で変調された出力光（クロック光）は合波器（１１０）で合波された後、光ファイバ伝送路のチャネル（１１１）で受信者まで伝送される。

［式１］　$\delta \leqq 0.8/N$

［式２］　$2\delta L^2N^2/Nn > 0.1$

ここで、Ｎは信号光の光子数、δは信号光の変調度、Ｌは伝送路の損失、Ｎｎは受信装置の雑音レベル（予め測定により既知）である。

【００２１】

受信者側では波長分波器（１１２）でクロック光と信号光を分離する。クロッ

ク光は光検出器（１２１）で電気信号に変換された後クロック再生回路（１２２）で波形整形されてクロック信号に再生され、受信者側のクロックとなる。信号光はマンチェスター符号を復号するため、５０％－５０％の分波器（１１７）で２分され、一方を遅延器（１１８）で半クロック分だけ遅らせる。２分された各々の信号光は、２つの検出器の出力差を信号として出力するバランスドデテクタ（１１９）で検出され、復号される。この時のマンチェスター符号とその復号された波形の模式図を図２に示す。図中、Ａはマンチェスター符号（図１Ａ点の波形）、ＢはＡのマンチェスター符号に対して半周期遅らせたマンチェスター符号（図１Ｂ点の波形）、ＣはＡのマンチェスター符号とＢのマンチェスター符号との差、即ち、バランスドデテクタ（１１９）で復号された信号波形（図１Ｃ点の波形）である。マンチェスター符号は、出力されるスロットの後ろ半分を信号とすることで、図２に示す如く、“０”と“１”が絶対値が等しい正負の電圧信号に復号される。

【００２２】

バランスドデテクタ（１１９）で検出される信号光には雑音が重畳しており、バランスドデテクタ（１１９）の測定結果には揺らぎが存在する。この信号光の揺らぎを考慮した場合の受信者側における、“０”と“１”に復号された電圧信号、及び、多数回の測定によって得られる“０”と“１”の頻度分布、即ち、確率分布の模式図を図３に示す。（ａ）は揺らいでいる電圧信号の、或る瞬時の“０”と“１”に復号された電圧信号波形（図２のＣに相当）、（ｂ）は”０”の確率分布、（ｃ）は”１”の確率分布を示す。図３（ｂ）、（ｃ）において、横軸は復号された信号の大きさ、縦軸は頻度、即ち、信号が検出される確率である。バランスドデテクタ（１１９）は直流分を打ち消すため、バランスドデテクタ（１１９）で得られる“０”と“１”に復号された出力の各々の確率分布Ｐ（Ｖ）は、図３に示すように、互いに電圧値Ｖ＝０に対して対称になる。

【００２３】

バランスドデテクタ（１１９）で得られた信号は増幅器（１２０）で増幅された後、クロックごとに演算装置（１１５）でディジタル信号になって記憶装置（１１６）に記憶される。演算装置（１１５）は、送信者がいくつかの乱数を送り

終えた後で記憶装置（１１６）に記憶された信号の確率分布関数を計算し、計算された確率分布関数が図３に示す如く“０”、“１”に対応して２つのガウス型関数で近似できることを確かめる。確率分布に異常（例えば、分散の増減、対象性の劣化、ピーク値をとる電圧値の変化等）が発見されたときは、盗聴があった証であるから、この回に得た信号は捨てる。確率分布に異常が発見されない場合、盗聴がないと判定できるので、判別閾値V_{th}に基づいて各々のビットについてビット値の判別を行う。このとき、判別閾値V_{th}はビット値“０”と“１”で符号が異なり、絶対値が同じ有限の値$V_{th}=\pm mS$（Ｓは信号の振幅の平均値、ｍは０又は正数）を用いる。つまり、信号出力Ｖが$-mS$より小さいときビット値が１、mSより大きいとき０と判別し、$-mS$とmSの間にあるときは判別不能とする。雑音が大きいとき、判別閾値V_{th}の絶対値$|V_{th}|$を大きくする（ｍを大きくする）と判別できるビットは減るが、判別できたビットについては誤り率を小さくすることができる。この時、ｍ、即ち、判別閾値は、式７（後述説明する）や図６に基づいて、受信者の誤り率が５％以下になるように決める。

【００２４】

乱数列の送信が終わった後で、判別できたビットの位置を暗号鍵伝送路とは独立な伝送路、例えば、現行の光通信網や無線、電話等の古典的な通信路を用いて送信者に連絡する。受信者が判別不能としたビットと誤って判別したビットとを捨て、判別できたビットだけを取り出すことにより、送信者と受信者は誤りの少ない乱数列を共有できる。この共有できた乱数列を暗号鍵とする。

【００２５】

もし、盗聴者が通信路から光を一部取り出したとしても、受信者と盗聴者の間の雑音に相関がないので受信者がどのビットを判別できるかを盗聴者は予め知ることはできない。そのため、盗聴漏れを防ぐために、盗聴者は判別閾値を０にして全てのビットについて判別を行わなければならず、受信者の得た誤りの少ないビットは盗聴者にとっては誤りを含んだものになる。このため、雑音が大きい場合には誤り率が大きくなって、受信者の情報量に対して盗聴者の情報量は小さく、効果的な盗聴ができない。盗聴者が送られてくる光を全て吸収して判別を行い、結果を受信者に送ることも可能だが、その場合でも盗聴者の誤り率が１０％以

上になるよう設定してあるので（式１を満足するように送信信号光の光強度と変調度を設定）、盗聴者の判別は誤りを含み、受信者の誤り率が異常に増加して盗聴者の存在が暴露される。盗聴が検出された場合には暗号鍵の生成を中止し、別の伝送路を用いて新たに暗号鍵の生成、配布をもう一度最初からやり直す。

【００２６】

他の実施の形態として、上記の暗号鍵配布方法に加えてさらに安全な暗号鍵を共有するために、上記暗号鍵生成プロトコルに加えて、誤り訂正や秘匿性増強のために古典的な情報を送信者と受信者の間で交換する。これらの情報はクロック信号と同じ波長帯の光を用いて双方向通信を行う。送信側の光強度と変調度とを暗号鍵と同時に送って、受信側で、受信した送信側の光強度情報と既知の伝送路損失から予想される受信光の光強度期待値を計算し、その結果と実際に受信した受信光の光強度とを比較し、計算値と実測値との差に応じて受信側で伝送路の異常の有無を検知する。検知した伝送路の異常程度を手がかりに盗聴の有無を判断し、暗号鍵配布を中止するか又は続行するかを決定する。この時の演算装置の動作は、図８の流れ図に従う。

【００２７】

送信者の光強度と変調度、受信者の判別閾値は次のように決められる。受信者の得る信号の確率分布が下記の式３、式４で与えられるガウス型であるとする。

［式３］　$P(V)=(2\pi\sigma^2)^{-1/2}\exp[-(V-S)^2/(2\sigma^2)]$

（ビット値０が送信されたとき）

［式４］　$P(V)=(2\pi\sigma^2)^{-1/2}\exp[-(V+S)^2/(2\sigma^2)]$

（ビット値１が送信されたとき）

ここで、Ｓは確率変数Ｖの平均値、即ち、信号の振幅（Ｖ）の平均値、σは信号の振幅の標準偏差である。

このとき、信号対雑音比β^2は$\beta=S/\sigma$と表せる。

【００２８】

式３に対して$y=(V-S)/\sigma$、式４に対して$y=(V+S)/\sigma$とし、式３、式４を標準化すると式３、式４は$(2\pi)^{-1/2}\exp[-y^2/2]$となるから、ｙがｘ以上となる確率Ｑ（ｘ）は、下記式５で表される。

[式５]　$Q(x)=(2\pi)^{-1/2}\int_{x}^{\infty} \exp[-y^2/2]dy$

【００２９】

従って、受信者が判別閾値V_{th}＝±ｍＳを用いてビット値を正しく判別する確率はＱ（（ｍ－１）β）、誤って判別する確率はＱ（（ｍ＋１）β）となる。これより受信者がビット値を判別する確率Ｆは下記式６で表される。

[式６]　Ｆ＝Ｑ（（ｍ－１）β）＋Ｑ（（ｍ＋１）β）

判別した結果が誤りである確率、即ち、誤り率Ｐｅは下記式７のようになる。

[式７]　Ｐｅ＝Ｑ（（ｍ＋１）β）／Ｆ

受信者と盗聴者の雑音には相関がないので、盗聴者は受信者がどのビットで判別をするか予め知ることはできない。そのため、盗聴漏れがないようにするためには、盗聴者は判別閾値V_{th}を０（ｍ＝０）にして全てのビットについて判別を行わなければならない。盗聴者の誤り率P^Eは盗聴者の信号対雑音比がB^2のとき、下記式８で与えられる。

[式８]　$P^E=Q(B)$

盗聴者が吸収－再送を行うと受信者の誤り率は下記式９に示すように変化する。

[式９]　$Pe'=P^E(1-Pe)+(1-P^E)Pe$

式９から分るように、盗聴者のいないときの受信者の誤り率Ｐｅが５％になるように判別閾値V_{th}を選ぶと、盗聴者の誤り率P^Eが１０％のとき受信者の誤り率は１４％となり、盗聴者がいると受信者の誤り率がほぼ３倍になる。このように、いかなる盗聴者にとって誤り率P^Eが１０％を越えるように光強度と変調度を設定する、即ち、誤り訂正が不可能になる誤り率となるように光強度と変調度を設定すると、吸収－再送を行う盗聴者の存在は誤り率の異常な増加から検出できる。

【００３０】

ここで、受信者の誤り率を５％、盗聴者の誤り率を１０％としたのは、誤り率が１０％を超えると誤り訂正が不可能になるという事実を考慮して定めた。受信者の誤り率は、誤り訂正が可能な１０％未満であれば何パーセントでもよいが、

１０％に近いと誤り訂正が難しく、また、１％のように誤り率を低くすると送信が難しくなるので、送信と誤り訂正の容易性・困難性を考慮して５％とした。もちろん受信者の誤り率が１０％未満であれば５％以外、例えば、４％、６％等、でもよいことは云うまでもない。盗聴に対して安全であるためには、盗聴者が誤り訂正ができないようにすればよいから、盗聴者の誤り率を１０％以上とすればよい。誤り率が１０％以上で、盗聴者が最も有利な状況（受信者にとっては最も不利な状況）となるのは誤り率が１０％のときであるから、盗聴者の誤り率を１０％とすれば、受信者が最も不利な状況においても盗聴に対して安全であるための光強度、変調度、判別閾値を決めることができるので、盗聴者の誤り率を１０％とした。

【００３１】

傍受型の攻撃に対する安全性を求めるために、以下のように暗号鍵の伝送レートＲを計算する。これは、受信者が判別できたビット列から安全な暗号鍵を取り出せる割合を表すもので伝送レートＲが０より大きいことが暗号鍵の伝送に必要である。暗号鍵の伝送レートＲは送信者と受信者の間のシャノン情報量I_{AB}＝１＋Ｐｅｌｏｇ$_2$Ｐｅ＋（１－Ｐｅ）ｌｏｇ$_2$（１－Ｐｅ）から、誤りの訂正のために失われるビットの割合Ｐｅと盗聴者に流れる情報の割合（１－Ｐｅ）Ｔを引いたものになる。即ち、伝送レートＲは下記式１０で表される。

［式１０］　$R = I_{AB} - Pe - (1-Pe)T$

ただし、Ｔは受信者の得たビット列のｉ番目がｋである確率ｐ（ｋ）と、受信者と盗聴者のビット列のｉ番目がそれぞれｋ，ｌである確率ｐ（ｋ，ｌ）を使って

［式１１］　$T = 1 + \log_2 [p(0,0)/p(0) + p(0.1)/p(0) + p(1,0)/p(1) + p(1,1)/p(1)]$

と表せる。確率ｐ（ｋ，ｌ）は、

$p(0,0) = p(1,1) = (1-P^E)$

$p(0,1) = p(1,0) = P^E$

であり、ｐ（０）＝ｐ（１）＝１／２を仮定しているから、

$T = 1 + \log_2 [1 - 2P^E + 2(P^E)^2]$

となる。結局、暗号鍵の伝送レートＲは受信者と盗聴者の誤り率を用いて

［式１２］　$R=1+Pe\log_2 Pe+(1-Pe)\log_2(1-Pe)-Pe-(1-Pe)\{1+\log_2[1-2P^E+2(P^E)^2]\}$

と書ける。

【００３２】

図４に傍受型の攻撃に対して安全な暗号鍵配布を行うために必要な受信者の誤り率Ｐｅと盗聴者の誤り率P^Eの領域を示す。図中の曲線は式１２においてＲ＝０を満足する曲線である。曲線の上方は式１２のＲ＞０を満たす領域で、判別できたビット列から暗号鍵を取り出せる割合が正となる領域、即ち、暗号鍵の配布が可能な領域である。曲線の下方は式１２のＲ＜０を満たす領域で、判別できたビット列から暗号鍵を取り出せる割合が負となり、ビット列から暗号鍵を取り出せない領域、即ち、暗号鍵の配布が不可能な領域である。図４より、盗聴者の誤り率を１０％（誤り訂正が不可能な誤り率のうちで盗聴者がもっとも有利な誤り率）とすると、受信者の誤り率を５％以下にすれば傍受型の攻撃に対しても安全といえる。従って、前述した、吸収－再生型の攻撃に対して安全である条件を考慮すると、吸収－再生型の攻撃と傍受型の攻撃の両方に対して安全であるためには受信者の誤り率を５％以下にすればよい。

【００３３】

盗聴者の誤り率P^Eは式８で与えられ、信号対雑音比と盗聴者の誤り率P^Eとの関係は図５に示すようになる。図５から分るように、盗聴者の誤り率P^Eが１０％以上となるためには、盗聴者の信号対雑音比は１．６（２ｄＢ）以下であれば良い。盗聴者がもっとも有利な状況として、盗聴者が送信端にいてショット雑音で制限される理想的な検出器を持っているとする。伝送路に入射する平均光子数がＮで、変調によって光子数がＮ（１±δ）のように変化するとき、信号対雑音比は２δＮになる。従って、盗聴者の信号対雑音比を１．６（２ｄＢ）以下とするためには、変調度δは下記式１を満たすように決めればよい。

［式１］　$\delta \leqq 0.8/N$

一方、受信者が０でない判別閾値V_{th}（$V_{th}=\pm mS$（Ｓは信号の振幅の平均値、ｍ≠０）を用いたときの判別閾値と受信者の誤り率との関係をさまざまな信

号対雑音比の値について式７により計算した結果を図６に示す。図中、縦軸は受信者の信号対雑音比、横軸は判別閾値V_{th}＝±ｍＳのｍ値を示す。曲線５１、５２、５３、５４、５５、５６は信号対雑音比がそれぞれ７．８ｄＢ、２．６５ｄＢ、－３．２８ｄＢ、－９．２５ｄＢ、－１５．１ｄＢ、－２１．４ｄＢのときの判別閾値と誤り率の関係を示す曲線である。図６によれば、信号対雑音比が－１５．１ｄＢの場合（曲線５５）と、－２１．４ｄＢの場合（曲線５６）はｍを大きくしても、即ち、判別閾値を大きくしても受信者の誤り率を５％以内にできない。信号対雑音比が－９．２５ｄＢ（曲線５４）であれば受信者の誤り率が５％以内（吸収－再生型、傍受型の何れの攻撃に対しても安全な誤り率）になるように判別閾値を選ぶことができる。このようことから、受信者の誤り率を５％以内にするには受信者の信号対雑音比が－１０ｄＢ以上必要なことが分かる。また、信号対雑音比が－９．２５ｄＢ（曲線５４）のとき、判別閾値V_{th}は平均信号強度Ｓの１２倍程度以上（ｍ≧１２）にする必要がある。信号対雑音比が－３．２８ｄＢ（曲線５３）の場合は、判別閾値V_{th}は平均信号強度の３倍程度以上（ｍ≧３）であればよい。判別閾値を大きくすると誤り率は低下するが同時に判別するビット数も減少するので、誤り率に関する条件を満たしている限り判別閾値はできるだけ低い方が良い。受信者の受け取る平均光子数をＮｒ、雑音強度をＮｎとすると、信号対雑音比は$2\delta Nr^2/Nn$となる。伝送路の損失Ｌのために$Nr=LN$は、伝送路に入射する信号光の平均光子数Ｎより小さくなる。前述したように、受信者の誤り率を５％以内にするには受信者の信号対雑音比が－１０ｄＢ以上必要であるから、受信者の信号対雑音比が－１０ｄＢ以上（０．１以上）になる、つまり、

［式２］　$2\delta L^2N^2/Nn>0.1$

となるように伝送路に許される損失Ｌ、伝送路に入射する信号光の平均光子数Ｎ及び変調度δを決める。ここで、雑音レベルＮｎは予め測定して求めておく。

【００３４】

上記の実施の形態では、“０”と“１”の信号に対する検出器出力の確率分布が対称になるようにマンチェスター符号を用いたが、２値位相変調を用いても良い。この場合、得られる信号対雑音比が上記実施の形態と異なるので変調度、判

別閾値は誤り率の条件を満たすように変更する。

【００３５】

【発明の効果】

以上説明したように、本発明は、暗号鍵配布において、理論上安全性が保証できる盗聴者の信号対雑音比の限度が明確になっており、また、安全な暗号鍵配送を行うための伝送路損失と送信光の光強度及び変調度との関係も明確になっているため、システムの設計が現実の条件に則して行える。さらに、伝送路の異常を判断する方法も与えらている。このため、本発明においては、現在の光通信網を利用できるコヒーレント光を用いて、安全な暗号鍵配布システムを提供できる。

【図面の簡単な説明】

【図１】　本発明の実施の形態の構成図。

【図２】　マンチェスター符号とその復号法を示す図。

【図３】　信号光の揺らぎを考慮した場合の復号された電圧信号、及び、多数回の測定によって得られる電圧信号の確率分布を示す模式図。

【図４】　傍受型の攻撃に対して安全な暗号鍵配布を行うために必要な受信者の誤り率と盗聴者の誤り率の領域を示す図。

【図５】　判別閾値が０のときの信号対雑音比と盗聴者の誤り率との関係を示す図。

【図６】　０でない判別閾値を用いたときの判別閾値と受信者の誤り率との関係を示す図。

【図７】　演算装置の動作を示す流れ図。

【図８】　演算装置の動作を示す流れ図。

【符号の説明】

１１　クロック発生器

１２　乱数発生器

１３　符号化器

１４　第１の光源

１５　第１の変調器

１６　減衰器

１７　光強度モニタ

１８　第２の光源

１９　第２の変調器

１１０　合波器

１１１　伝送路

１１２　波長分波器

１１３　クロック再生装置

１１４　復号・検出器

１１５　演算装置

１１６　記憶装置

１１７　分波器

１１８　遅延器

１１９　バランスドデテクタ

１２０　増幅器

１２１　光検出器

１２２　クロック再生回路

５１　信号対雑音比７．８ｄＢの曲線

５２　信号対雑音比２．６５ｄＢの曲線

５３　信号対雑音比－３．２８ｄＢの曲線

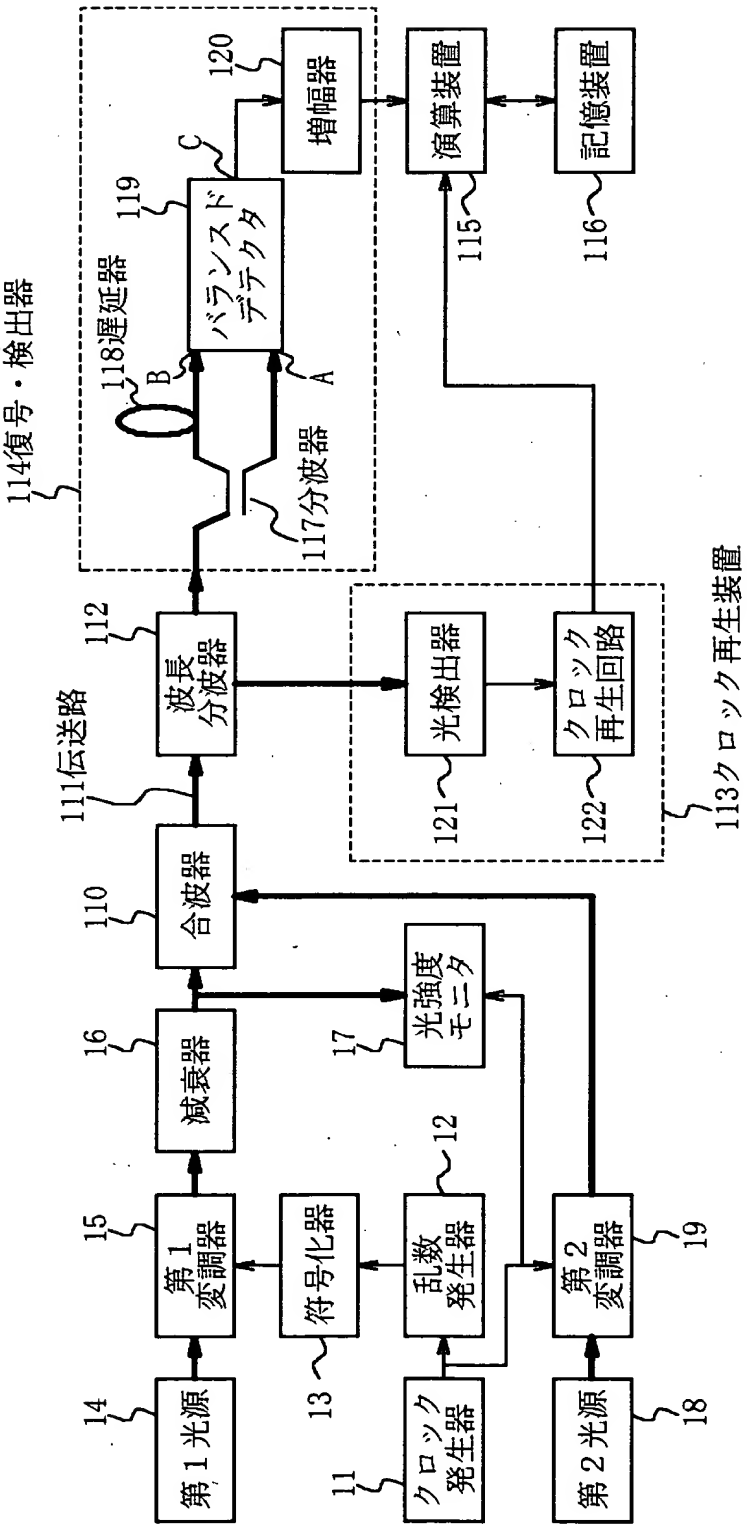
５４　信号対雑音比－９．２５ｄＢの曲線

５５　信号対雑音比－１５．１ｄＢの曲線

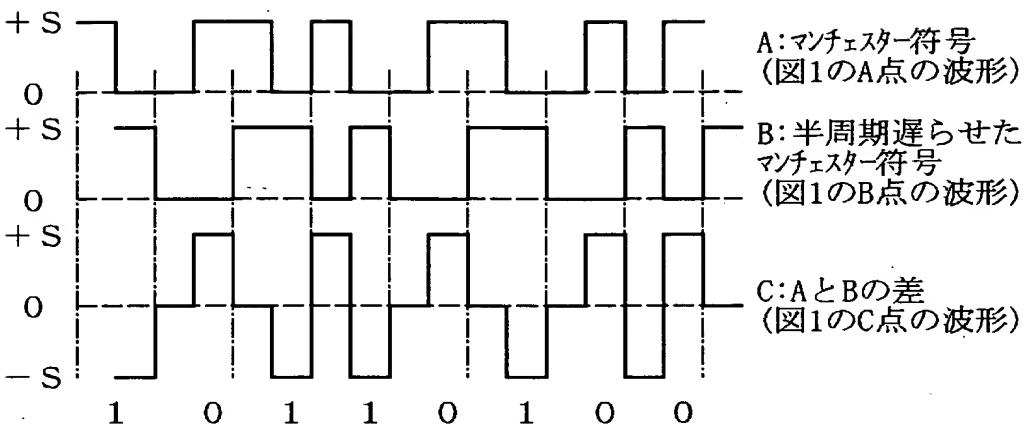
５６　信号対雑音比－２１．４ｄＢの曲線

【書類名】　　図面

【図１】

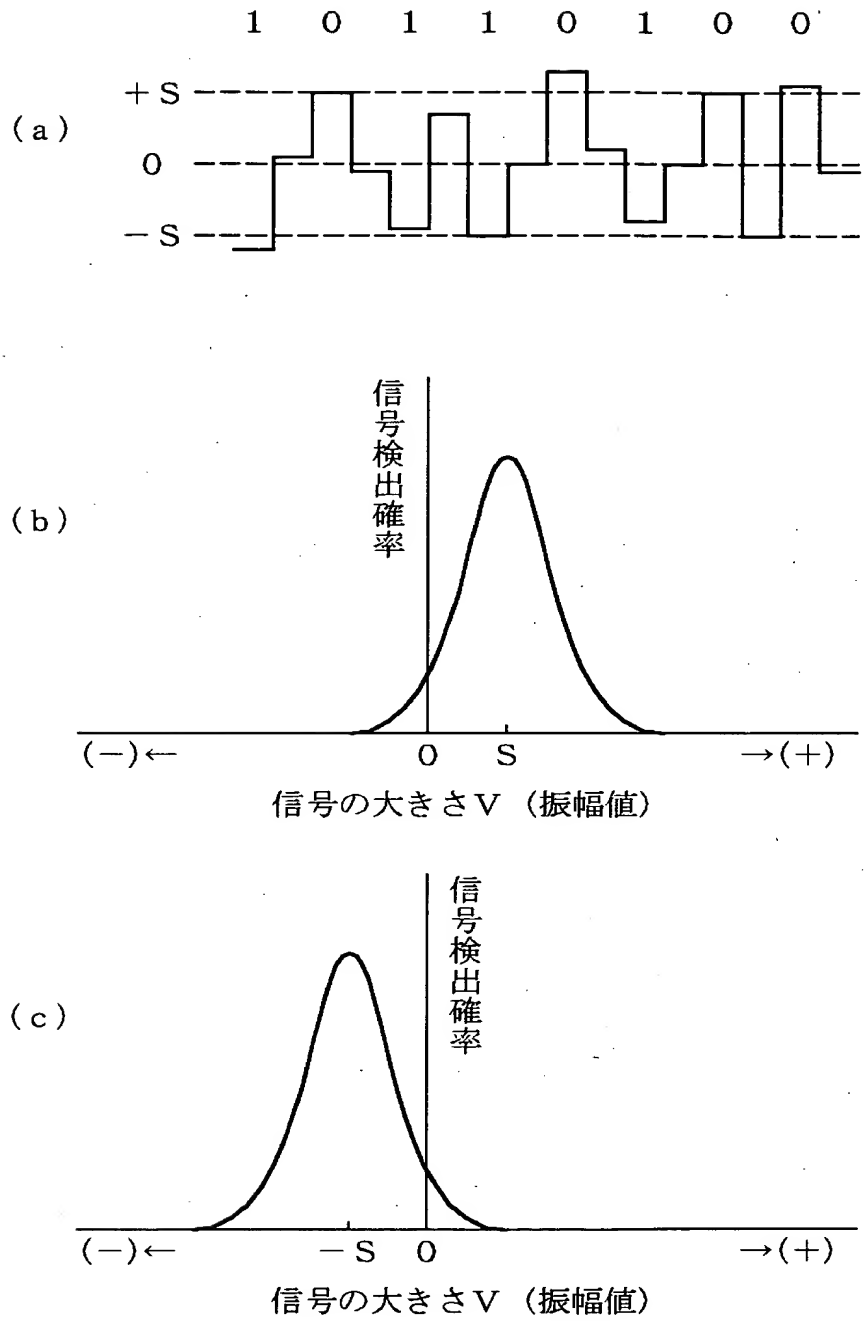

第１光源
14
第１変調器
15
減衰器
16
合波器
110
波長分波器
112
111伝送路
114復号・検出器
118遅延器
B
A
バランスドデテクタ
119
C
増幅器
120
117分波器
演算装置
115
記憶装置
116
光検出器
121
クロック再生回路
122
113クロック再生装置
光強度モニタ
17
符号化器
13
乱数発生器
12
クロック発生器
11
第２変調器
19
第２光源
18

【図２】

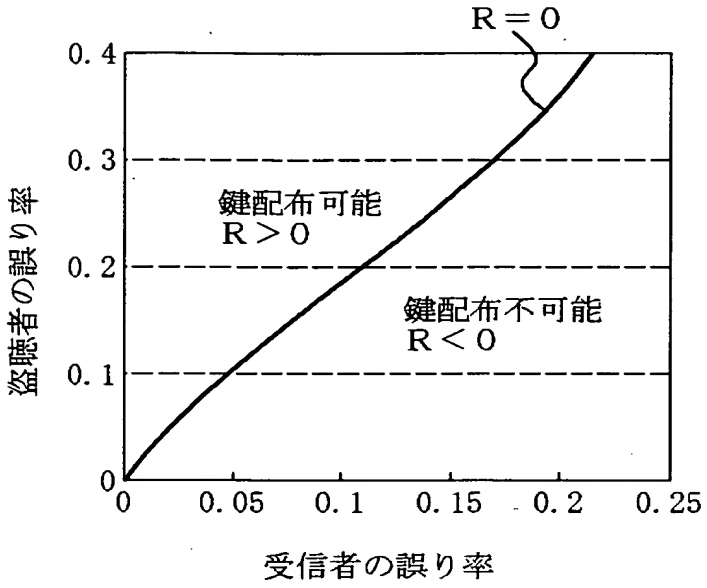


出証特２００１－３０５８１９２

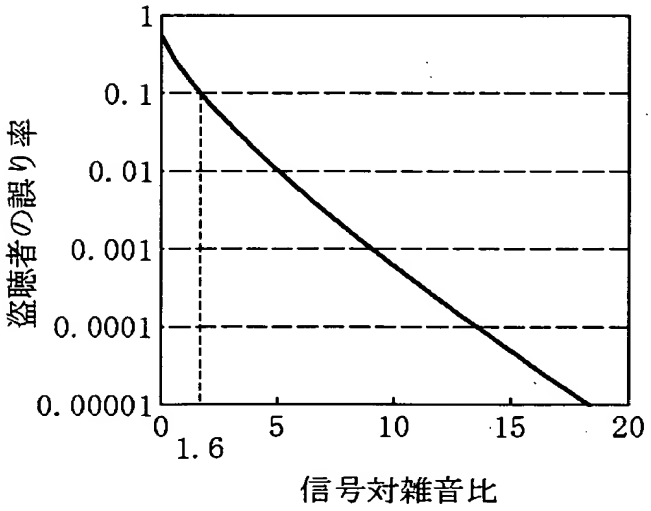
【図３】


1 0 1 1 0 1 0 0
(a)
+S
0
−S
(b)
信号検出確率
(−)←
0
S
→(+)
信号の大きさＶ（振幅値）
(c)
信号検出確率
(−)←
−S
0
→(+)
信号の大きさＶ（振幅値）

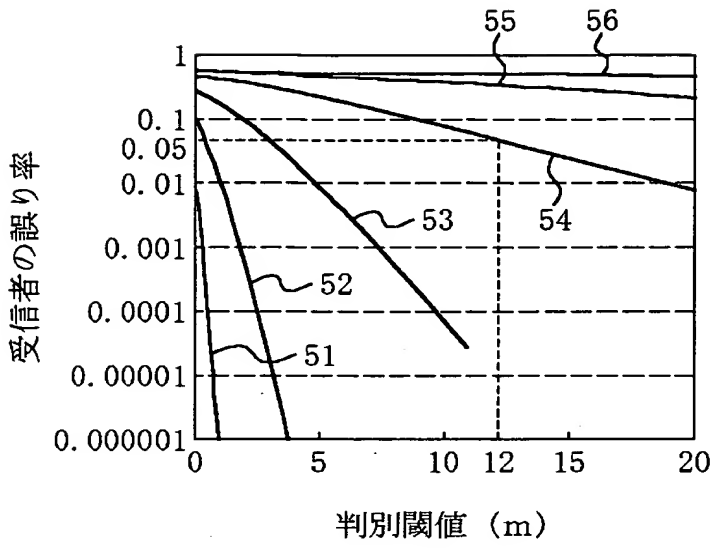
【図４】


R＝０
0.4
0.3
0.2
0.1
0
鍵配布可能
R＞０
鍵配布不可能
R＜０
盗聴者の誤り率
0
0.05
0.1
0.15
0.2
0.25
受信者の誤り率

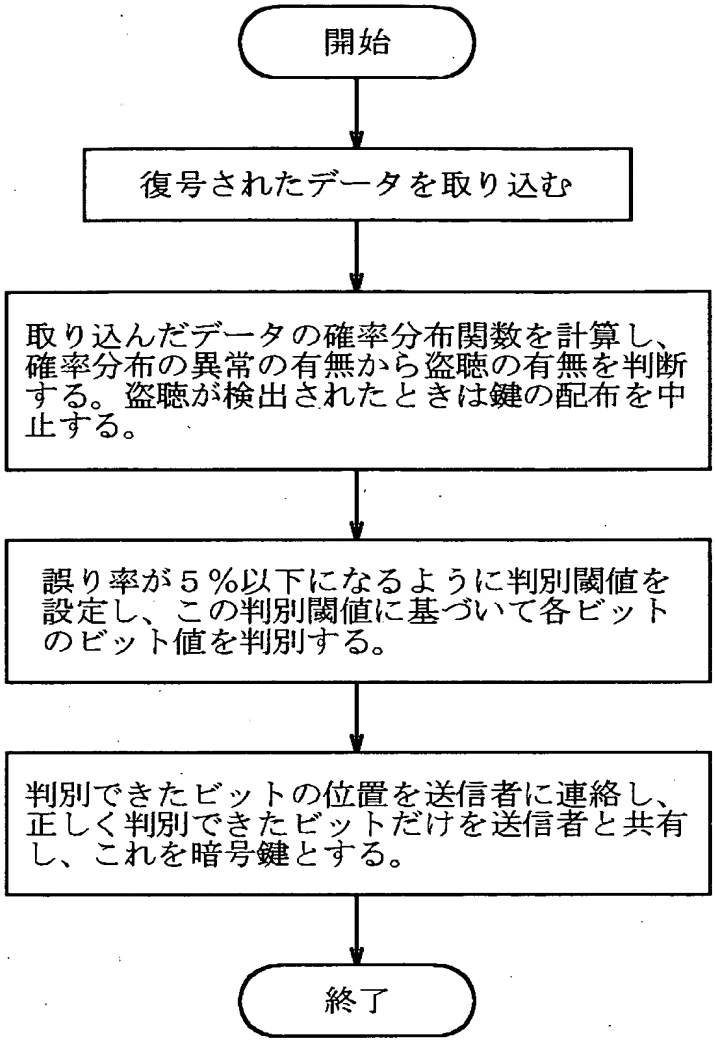
【図５】


1
0.1
0.01
0.001
0.0001
0.00001
盗聴者の誤り率
0
1.6
5
10
15
20
信号対雑音比

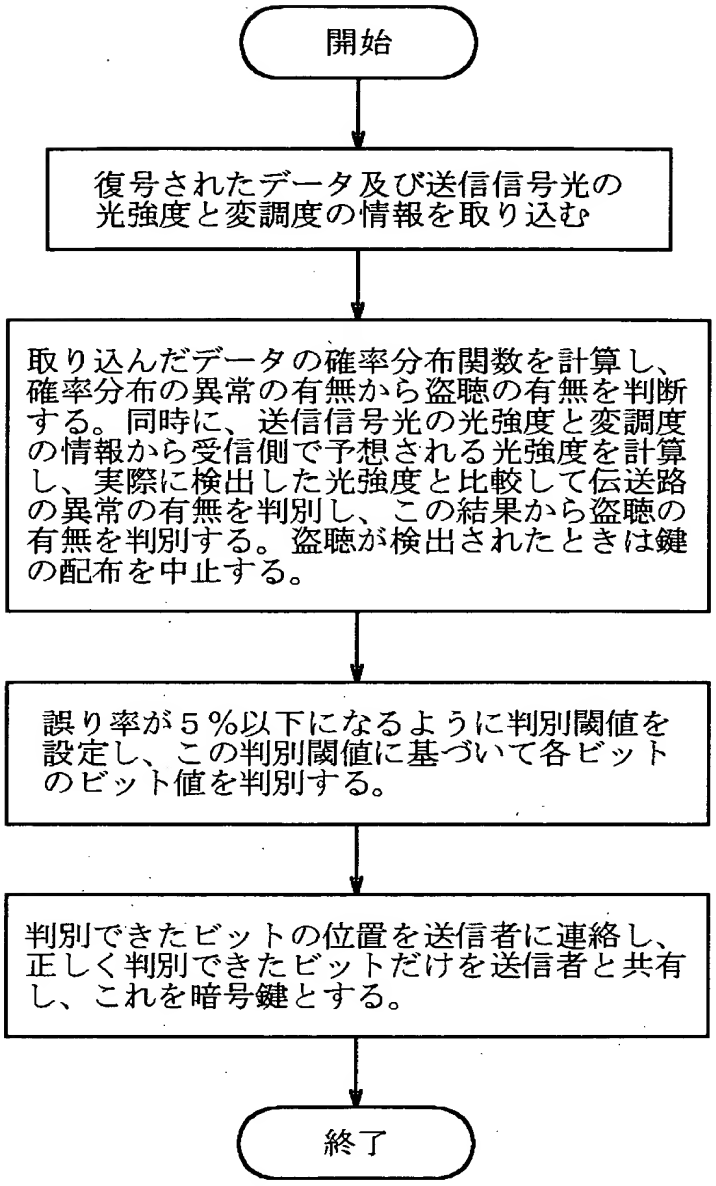
【図６】


55
56
1
0.1
0.05
0.01
0.001
0.0001
0.00001
0.000001
受信者の誤り率
53
54
52
51
0
5
10
12
15
20
判別閾値（m）

【図７】


開始
復号されたデータを取り込む
取り込んだデータの確率分布関数を計算し、確率分布の異常の有無から盗聴の有無を判断する。盗聴が検出されたときは鍵の配布を中止する。
誤り率が５％以下になるように判別閾値を設定し、この判別閾値に基づいて各ビットのビット値を判別する。
判別できたビットの位置を送信者に連絡し、正しく判別できたビットだけを送信者と共有し、これを暗号鍵とする。
終了

【図８】


開始
復号されたデータ及び送信信号光の光強度と変調度の情報を取り込む
取り込んだデータの確率分布関数を計算し、確率分布の異常の有無から盗聴の有無を判断する。同時に、送信信号光の光強度と変調度の情報から受信側で予想される光強度を計算し、実際に検出した光強度と比較して伝送路の異常の有無を判別し、この結果から盗聴の有無を判別する。盗聴が検出されたときは鍵の配布を中止する。
誤り率が５％以下になるように判別閾値を設定し、この判別閾値に基づいて各ビットのビット値を判別する。
判別できたビットの位置を送信者に連絡し、正しく判別できたビットだけを送信者と共有し、これを暗号鍵とする。
終了

【書類名】　　要約書

【要約】

【課題】光ファイバ通信網に適合したコヒーレント光を用いて、安全性の保証された暗号鍵配布システムを提供する。

【解決手段】送信者は、受信側で対称な確率分布を持つように乱数を符号化し、送信光出力の強度と変調を、盗聴者が送信端で最良の受信機を用いたときでも盗聴者の信号対雑音比が２ｄＢ以下になるように設定すると同時に、受信者の信号対雑音比がー１０ｄＢ以上になるように設定して送信する。受信者は一組の乱数が伝送された後、得られた信号の確率分布を計算して判別閾値を求め、確率分布に異常があるとき盗聴があったと判断し、暗号鍵の伝送をやり直す。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－２５２６５６
受付番号	５００００１０６９０６５
書類名	特許願
担当官	第八担当上席　００９７
作成日	平成１２年　８月２４日

＜認定情報・付加情報＞

【提出日】　平成12年 8月23日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社